UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO.	: 7,093,130 B1
APPLICATION NO.	: 09/490354
DATED	: August 15, 2006
INVENTOR(S)	: Kobayashi et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title Page; item (56)

In the Issued Patent:

Under References Cited, U.S. Patent Documents, before “5,629,980”, please insert --5,557,518 A* 9/1996 Rosen--.

Under References Cited, U.S. Patent Documents, after “2002/0116616”, please insert --2002/0095383 A1* 7/2002 Mengin et al.--.

Column 20, line 17, between “method” and “first” please insert the following: --system and ticket of the present invention are secure, and just how everything “comes together” to offer all the many benefits enumerated in section 1.

Consider things from this viewpoint: The computer of the ticket consumer is producing something -- the one-way function, or hash, of an (essentially) random number initially known only to itself -- that the ticket provider’s computer cannot produce -- at least initially at a time before ticket redemption. The ticket provider’s computer could produce this one-way hash function if only it had the random number, but initially it does not have this number.

The computer of the ticket producer, receiving across the network the one- way hash function from the consumer’s computer where it was produced, proceeds to produce something -- a signed digital signature -- that the consumer’s computer cannot produce. The consumer’s computer might be able to do this signing procedure itself if it but had the secret signature key of the producer’s computer; but it does not.

PATENT NO. : 7,093,130 B1
APPLICATION NO. : 09/490354
DATED : August 15, 2006
INVENTOR(S) : Kobayashi et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Issued Patent:

Note immediately that a party intercepting some, or all, communications traffic on the network concerning the digital ticket is still unable to determine either (i) the random number of the computer of the ticket consumer (**R**, in the preceding sections) or (ii) the signature key (**s**, in the preceding sections), of the ticket producer's computer.

The consumer's computer , receiving across the network from the producer's computer its own (previously transmitted) one-way hash function now signed, simply appends the original random number, and stores the composite away as the digital ticket.

When the ticket is redeemed then, for the first time ever, either the producer's computer or, more likely, a gate keeper's computer in privity of relationship with the producer's computer at least as regards how to decrypt the digital signature of the producer's computer, will immediately have access to -- for the--.

Column 24, line 19, please delete "R_2evenR", and insert --R_2evenR_1-- therefor.

UNITED STATES PATENT AND TRADEMARK OFFICE

CERTIFICATE OF CORRECTION

PATENT NO. : 7,093,130 B1 Page 3 of 3
APPLICATION NO. : 09/490354
DATED : August 15, 2006
INVENTOR(S) : Kobayashi et al.

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

In the Issued Patent:

Column 25, line 63, delete "$\forall C : R_i$", and insert --$\ni C : R_i$-- therefor.

Column 35, line 57, after "fourth-calculated", please delete "Sign (s, I" and insert --Sign (s, I ‖-- therefor.

Signed and Sealed this

Eighth Day of April, 2008

Jon W. Dudas

JON W. DUDAS
Director of the United States Patent and Trademark Office